DHCP and Router Advertisement Options for Encrypted DNS Discovery

https://tools.ietf.org/html/draft-btw-add-home

January 2021

M. Boucadair (Orange)
T. Reddy (McAfee)
D. Wing (Citrix)
N. Cook (Open-Xchange)
Tommy Jensen (Microsoft)

Overall Approach

- Rely upon existing mechanisms to distribute DNS server information: DHCP, DHCPv6, and RA

- Typical communication flow:
  - Clients ask for one or more Encrypted DNS (e.g., DoT, DoH) by setting dedicated flags in the options
  - Servers reply with ADN(s), a list of IP addresses, and a port number, if the requested encrypted DNS is supported
    - RECOMMENDED to return both an ADD and a list of IP addresses
    - One or more Encrypted DNS types may be returned
    - These services may listen on the same or distinct IP addresses
    - Alternate port numbers can be returned when default port are not in use
    - If a list of IP addresses is returned, that list is ordered

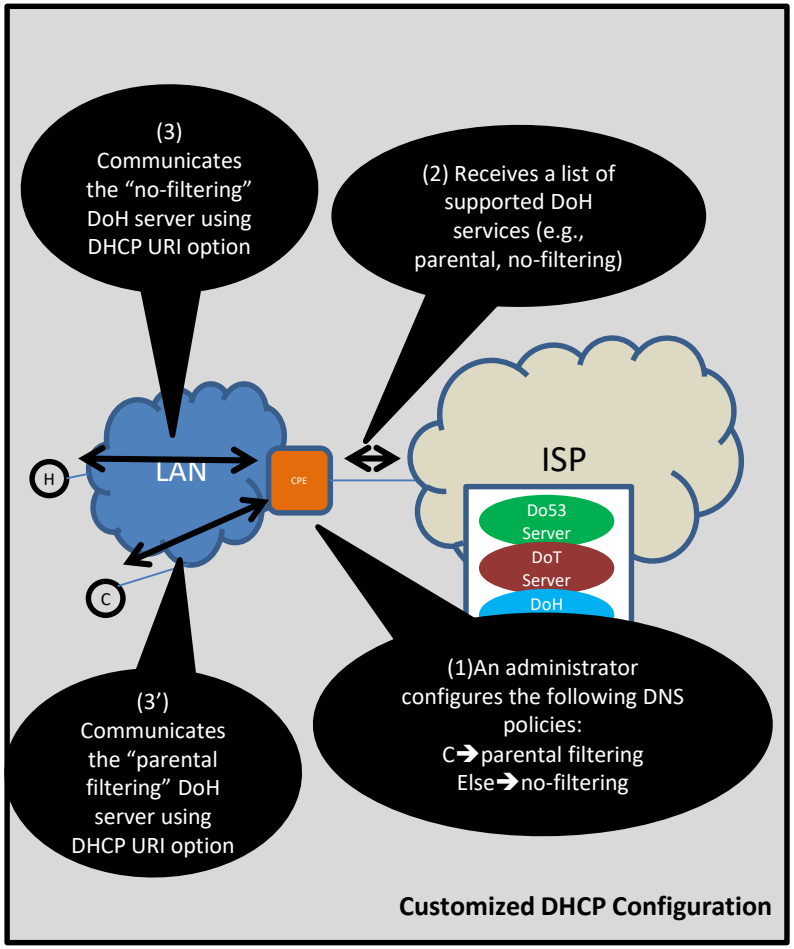
Main Changes Since IETF#108

- A list of IP addresses instead of relying upon legacy DNS options
- Generalize the specification
  - Remove deployment considerations
- Position the draft vs. DEER

- TBC

Question #1: URI Templates in RA/DHCP?

- There are some trade-offs
  - Some Issues
    - Create a dependency between DHCP servers (access routers) and DoH resolvers
    - May increase the size of RA/DHCP messages
  - Some advantages
    - There is no standard means to retrieve such information from the DoH server
    - Clients can immediately use the service(s)
    - No need for extra queries to retrieve the URIs
    - Allows for customized (local) configuration



Suggestion:

- Define RA/DHCP Options to convey URI Templates
- These options, when available, take precedence over RESINFO/DEER

Question #2: No ADN is Returned

- Accomodate cases where an IP address is used as a reference identifier
- Should we discuss this case?

Suggestion:

- Add text to the draft to cover this case

Question #3: No @List is Returned

- If the client receives a Do53 @List and an ADN, should the client use that list to resolve the ADN or should that list be assumed as locators of the encrypted?

Suggestion:

- Recommend to always return a list of @, unless Do53 and encrypted DNS terminate on the same @

Question

Question

Next Steps

- Consider adopting this document as a WG item

- Questions?